OIPE JC109
APR 10 2003
PATENT & TRADEMARK OFFICE

AF/3621

#9
J. Walden
4/16/03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of:)Attorney Docket No.: F-190

Robert A. Cordery et al.)Group Art Unit: 3621

Serial No.: 09/650,177)Examiner: C. Hewitt II

Filed: August 29, 2000)Date: April 4, 2003

Confirmation No.: 9743

RECEIVED
APR 1 5 2003
GROUP 3600

Title: SECURE USER CERTIFICATE FOR ELECTRONIC COMMERCE EMPLOYING VALUE METERING SYSTEM

Assistant Commissioner for Patents
Washington, D.C. 20231

APPELLANT'S BRIEF ON APPEAL

Sir:

This is an appeal pursuant to 35 U.S.C. § 134 and 37 C.F.R. §§ 1.191 et seq. from the final rejection of claims 35 and 36 of the above-identified application mailed October 29, 2002. The fee for submitting this Brief is $320.00 (37 C.F.R. § 1.17(c)). Please charge Deposit Account No. **16-1885** in the amount of $320.00 to cover these fees. The Commissioner is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. **16-1885**. The Notice of Appeal was received by the U.S. Patent and Trademark Office on February 6, 2002. Enclosed with this original are two copies of this brief.

04/11/2003 YPOLITE1 00000126 161885 09650177
01 FC:1402 320.00 CH

I. Real Party in Interest

The real party in interest in this appeal is Pitney Bowes Inc., a Delaware corporation, the assignee of this application.

II. Related Appeals and Interferences

The appeal in the following related case may have a bearing on the Board's decision in this appeal:

U.S. Application Serial No. 09/650,176, filed August 29, 2000.

III. Status of Claims

Claims 35 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer (U.S. Patent No. 5,005,200) in view of Payne et al. (U.S. Patent No. 5,715,314).

IV. Status of Amendments

There are no amendments to the claim filed subsequently to the final rejection of October 29, 2002. Therefore, the claims as set forth in Appendix A to this brief are those as set forth before the final rejection.

V. Summary of Invention

Appellant's invention relates to a secure user certification system for electronic commerce that provides an accounting system for services provided. In electronic commerce, various parties conduct activities without face to face contact. As such, it is desirable for each party to any transaction to be able to determine and verify the authenticity of the other party to the transaction, as well as ensure sufficient security for any commerce conducted electronically. Such security services could include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like. To effectively implement the above, a party to an electronic commerce transaction requires access to a secure cryptographic device capable of securely implementing these cryptographic techniques. According to the present invention, a certificate meter provides certificate management services including use of cryptographically secured certificates. Payment for the processing and issuing, by the certificate authority, of the electronic certificates can be made using funds stored in the meter. Thus, the present invention provides a party to an electronic commerce transaction access to a secure cryptographic device, i.e., a certificate meter, associated with a certificate authority, while providing the certificate authority with a convenient payment system to allow the certificate authority to get paid for processing and issuing of the electronic certificates.

Additional features of the invention are discussed below in the Argument section of this Brief.

VI. Issues

A. Whether the subject matter defined in claims 35 and 36 would have been obvious over Fischer in view of Payne et al.

VII. Grouping of Claims

Claims 35 and 36 are grouped in the following groups:

Group I - Claims 35 and 36.

None of the claims stand or fall together. The reasons why the Appellants believe the claims to be separately patentable are set forth in the Argument section of this Brief.

VIII. Argument

As Appellant discusses in detail below, the final rejection of claims 35 and 36 is devoid of any factual or legal premise that supports the position of unpatentability. It is respectfully submitted that the rejection does not even meet the threshold burden of presenting a prima facie case of unpatentability. For this reason alone, Appellant is entitled to grant of a patent. In re Oetiker, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992).

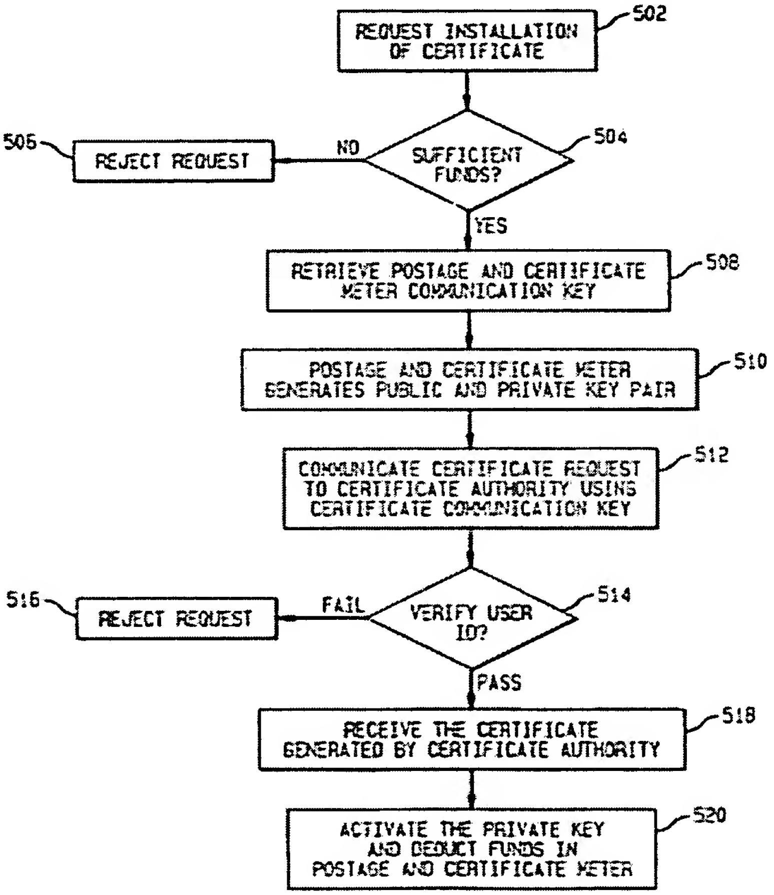
A. The subject matter defined by claims 35 and 36 would not have been obvious over Fischer in view of Payne et al.

Claim 35 is directed to a method for obtaining a cryptographic certificate. Specifically, claim 35 recites:

> A method for obtaining a cryptographic certificate, comprising the steps of:
>
> providing a register having funds stored therein;
>
> determining if sufficient funds are present in the register for obtaining the certificate;
>
> sending a certificate request to a certificate authority;
>
> receiving the cryptographic certificate from the certificate authority; and
>
> deducting funds from the register for obtaining the requested certificate.

Fig. 5 of the present specification, reproduced below, depicts a method of obtaining a cryptographic certificate according to the present invention. A request for installation of the certificate is initiated at 502. A determination is made at 504 if sufficient funds are available in the postage and certificate meter subsystem 218 to cover the charges associated with processing the request. If sufficient funds are not available the request is rejected at 506. If sufficient funds are available the postage and certificate meter communication key is retrieved at 508. The postage and certificate meter thereafter generates a public and private key pair at 510. Thus, the secure postage and certificate meter subsystem 218 securely generates the private key at 510. Thus, the private key is never available outside of the secure housing of the postage and certificate meter subsystem 218. In this preferred embodiment the private key is not known to anyone, including the certificate owner, therefore the postage and certificate meter can enforce charges for any use of the private key.

FIG. 5


REQUEST INSTALLATION OF CERTIFICATE
502
SUFFICIENT FUNDS?
504
NO
REJECT REQUEST
505
YES
RETRIEVE POSTAGE AND CERTIFICATE METER COMMUNICATION KEY
508
POSTAGE AND CERTIFICATE METER GENERATES PUBLIC AND PRIVATE KEY PAIR
510
COMMUNICATE CERTIFICATE REQUEST TO CERTIFICATE AUTHORITY USING CERTIFICATE COMMUNICATION KEY
512
VERIFY USER ID?
514
FAIL
REJECT REQUEST
516
PASS
RECEIVE THE CERTIFICATE GENERATED BY CERTIFICATE AUTHORITY
518
ACTIVATE THE PRIVATE KEY AND DEDUCT FUNDS IN POSTAGE AND CERTIFICATE METER
520

If less security is required and depending upon the configuration and needs of the system, the system can be modified such that the user can enter the private key into the postage and certificate meter subsystem 218. The certificate request is communicated to the certificate authority using the certificate communication key at 512. A determination is made at 514 to whether the user identification has been verified. If the verification fails, the request is rejected at 516. If the identity is verified the certificate generated by certification is received from the authority at 518. Thereafter, the certificate is installed in the postage and certificate meter subsystem 218 via the personal computer modem 220 and processor 212 and communication port 216 to the communication port 234 of the postage and certificate meter subsystem 218. Additionally at 520 the funds are deducted from the postage and certificate meter for the generation and the requested certificate which activates user's private key. (Specification, pages 17-18).

Thus, the certificate meter of the present invention is a secure cryptographic device with secret information that allows secure communication with a certificate authority such as a post office or other trusted third party and the capability to use, manage and execute various security services. The certificate meter of the present invention includes metering and accounting capability that allows convenient low cost payment of charges per use of a certificate.

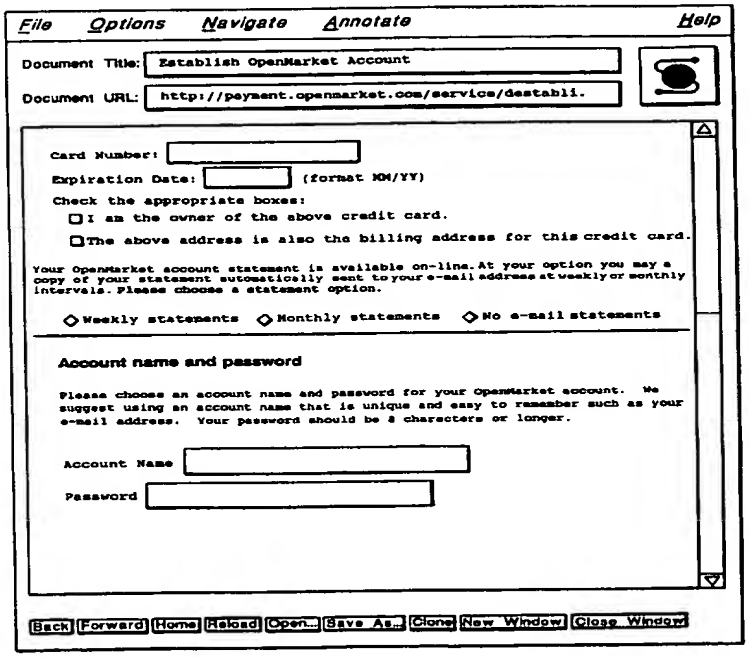
Fischer, in contrast, is directed to a public key cryptographic system with enhanced digital signature certification that authenticates the identity of the public key holder. Specifically, in Fischer, a trusted authority creates a digital message which contains the claimant's public key and the name of the claimant and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key. (Col. 3, lines 53-64). The system of Fischer provides the ability to specify a variety of attributes associated with the certification, such as specifying the authority or constraints which are conferred on the certifee by the certifier. (Col. 4, lines 56-62).

Thus, while Fischer discloses the use of certificates for providing security functions, as noted by the Final Rejection (page 3), there is no disclosure, teaching or suggestion in Fischer of providing a register having funds stored therein, determining if sufficient funds are present, and deducting funds from the register for obtaining a certificate, i.e., providing payment to the certificate authority for processing and issuing the certificate.

To overcome the above deficiency, the Final Rejection relies on the reference to Payne et al. Payne et al. is directed to network-based sales system that includes at least one buyer computer for operation by a user desiring to buy a product, at least one merchant computer, and at least one payment computer. The computers are inter-connected by a computer network. A purchase transaction begins when a user at buyer computer 12 requests advertisements (step 24) and buyer computer 12 accordingly sends an advertising document URL (universal resource locator) to merchant computer 14 (step 26). The merchant computer fetches an advertising document from the advertising document database (step 28) and sends it to the buyer computer (step 30). The user browses through the advertising document and eventually requests a product (step 32). This results in the buyer computer sending payment URL A to the payment computer (step 34).

The payment computer sends a payment confirmation document to the buyer computer, the payment confirmation document including an "open" link and a "continue" link (step 44). The confirmation document asks the user to click on a "continue" button if the user already has an account with the payment computer, or to click on an "open" button if the user does not already have an account and wishes to open one. If the user clicks on the "open" button (step 46), the buyer computer sends payment URL C to the payment computer (step 48), payment URL C being similar to payment URL A but also indicating that the user does not yet have an account. The payment computer creates a new account document (step 50) and sends it to the buyer computer (step 52). If the user clicks on the "continue" button (step 60), the buyer computer sends payment URL B to the payment computer (step 62), payment URL B being similar to payment URL A but also indicating that the user already has an account. The payment computer then instructs the buyer computer to provide the account name and password (steps 64 and 66), and the buyer computer prompts the user for this information by creating an account name prompt (example shown in FIG. 8) and a similar password prompt. The user enters the information (step 68) and the buyer computer sends the account name and password to the payment computer (step 70). The payment computer checks the settlement database to determine whether the user has unexpired access to the domain identifier contained in the payment URL (step 82). If so, the payment computer sends to the buyer computer a document providing an option either to repurchase or to use the previously purchased access (step 84). The user can respond to the recent purchase query document by choosing to access the previously purchased document (step 85) or to go ahead and buy the currently selected product (step 86). If the user chooses to buy the currently selected product, the payment computer calculates an actual payment amount that may differ from the payment amount contained in the payment URL (step 87). For example, the purchase of a product in a certain domain may entitle the user to access other products in the domain for free or for a reduced price for a given period of time. The payment computer then verifies whether the user account has sufficient funds or credit (step 76). If not, the payment computer sends a document to the buyer computer indicating that the user account has insufficient funds (step 78). (Col. 5, line 16 to Col. 7, line 20).

Thus, if Payne et al. teaches anything at all, it is merely a conventional network based sales system that utilizes a credit card account to pay for purchases made on-line. Although Payne et al. describes a step in which the payment computer verifies whether the user account has sufficient funds or credit (step 76 of Fig. 2G), there is no disclosure, teaching or suggestion in Payne of any type of register with funds stored therein. In fact, the only type of account ever described anywhere in Payne et al. is a conventional credit card account. Fig. 7 of Payne et al., reproduced below, illustrates a screen snapshot of a new account document that the payment computer sends to the buyer computer when the buyer desires to open a new account.



Document Title: Establish OpenMarket Account

Document URL: http://payment.openmarket.com/service/destabli.

Card Number:

Expiration Date: (format MM/YY)

Check the appropriate boxes:

□ I am the owner of the above credit card.

□ The above address is also the billing address for this credit card.

Your OpenMarket account statement is available on-line. At your option you may a copy of your statement automatically sent to your e-mail address at weekly or monthly intervals. Please choose a statement option.

◇ Weekly statements ◇ Monthly statements ◇ No e-mail statements

Account name and password

Please choose an account name and password for your OpenMarket account. We suggest using an account name that is unique and easy to remember such as your e-mail address. Your password should be 8 characters or longer.

Account Name

Password

FIG. 7

The buyer must complete this document to make a purchase utilizing the system of Payne et al. As illustrated, the user must input a credit card number and expiration date, and also indicate if they are the owner of the credit card. The user must also provide an account name and password that will be linked to the credit card account. (See Col. 6, lines 15-42). If the user already has an account, the user must provide the account name and password which were previously associated with the buyer's credit card when the account was opened. This credit card account is the only type of account disclosed, taught or suggested by Payne et al.

The Final Rejection states that it would have been obvious to combine Fischer and Payne et al. to arrive at the present invention, since by having an independent payment computer (e.g. a bank) verify a user's ability to pay prior to completing a transaction a merchant, such as a certificate authority, can guarantee compensation for service rendered. The present invention, however, is not directed to having an independent payment computer verify a user's ability to pay. As noted above, the present invention is directed to a certificate meter that can issue cryptographic certificates and provide payment for issuing the certificate. This is accomplished by providing a register having funds stored therein from which payment will be made upon receipt of the certificate. Even if Fischer and Payne et al. were combined, the combination still would not disclose, teach or suggest "providing a register having funds stored therein; determining if sufficient funds are present in the register for obtaining the certificate" and "deducting funds from the register for obtaining the requested certificate" as is recited in claim 35. As noted above, the only type of account disclosed in Payne et al. is a conventional credit card account. This is not the same as providing a register having funds stored therein. The combination of Fischer and Payne et al. would merely lead to a conventional credit card transaction. This is not the same as the present invention.

The Advisory Action mailed March 7, 2003, contends that "to one of ordinary skill it would have been obvious to use the register of Payne to obtain any good or service." As noted above, the payment system of Payne et al. is a conventional credit card payment system, and not a meter having a register with funds stored therein. Even if it were assumed, for argument's sake, that the system of Payne et al. was somehow equivalent to a register that contained funds, the Final Rejection has not provided any motivation for providing a secure user certification system for electronic commerce that provides an accounting system for services provided as in the present invention. "Determination of obviousness can not be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention. There must be a teaching or suggestion within the prior art, or within the general knowledge of a person of ordinary skill in the field of the invention, to look to particular sources of information, to select particular elements, and to combine them in a way they were combined by the inventor." ATD Corp. v. Lydall, Inc., 159 F.3d 534, 545 (Fed. Cir. 1998) (emphasis added). No such suggestion or motivation has been provided by the Final Rejection. The fact that the present invention was made by the Appellant does not make the present invention obvious; that suggestion or teaching must come from the prior art. See C.R. Bard, Inc. v. M3 Systems, Inc., 157 F.3d 1340, 1352 (Fed. Cir. 1998). See, e.g., Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051-1052 (Fed. Cir. 1988) (it is impermissible to reconstruct the claimed invention from selected pieces of prior art absent some suggestion, teaching, or motivation in the prior art to do so.)

Without using the present claims as a road map, it would not have been obvious to make the multiple, selective modifications needed to arrive at the claimed invention from these references. The rejection uses impermissible hindsight to reconstruct the present invention from this reference. See Ex parte Clapp, 227 U.S.P.Q. 972,973 (Bd. App. 1985) (requiring "convincing line of reasoning" to support and obviousness determination).

For at least the above reasons, Appellant respectfully submits that the final rejection as to claim 35 is in error and should be reversed. Claim 36 is dependent upon claim 35 and therefore the final rejection with respect to this claim should also be reversed.

Claim 36 is patentable, however, separate and apart from its dependency on claim 35 in that it includes novel limitations and a unique combination that would not have been obvious at the time of the invention. Specifically, claim 36 recites:

> The method of claim 35, comprising the further steps of:
>
> generating a first cryptographic key pair, wherein said certificate request includes at least a first public key of the first cryptographic key pair; and
>
> activating a first private key of the first cryptographic key pair.

Thus, as illustrated in Fig. 5 of the present specification (reproduced above), the postage and certificate meter of the present invention securely generates a public and private key pair at 510. The private key is, therefore, never available outside of the secure housing of the postage and certificate meter subsystem 218. In this preferred embodiment the private key is not known to anyone, including the certificate owner, therefore the postage and certificate meter can enforce charges for any use of the private key. At step 520, funds are deducted from the postage and certificate meter for the generation of the requested certificate which activates the user's private key. (Specification, pages 17-18).

The Final Rejection contends that Col. 3, lines 53-68, Col. 6., lines 36-65 and Col. 18, lines 32-68 teach the limitations of claim 36. Appellant respectfully disagrees.

Col. 3, line 53, to Col. 4, line 5, of Fischer state:

> The trusted authority creates a digital message which contains the claimant's public key and the name of the claimant (which is accurate to the authority's satisfaction) and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key (which enables verification of the authority's signature) and to the extent that the recipient trusts the authority.
>
> Certificates can be thought of as brief messages which are signed by the trusted authority, and which contain, either explicitly or implicitly, a reference to the public-key which is being therein certified, and the identity of the public key's owner (creator). In such an implementation, if "C" has provided a certificate for "A"; then recipient "B" can trust the use of "A's" public key, provided that "B" trusts "C", and provided that "B" possesses "C's" certification of "A's" public key.

Col. 6, lines 36-65, of Fischer state:

> In an exemplary embodiment of the present invention, a certifier is permitted to assign with one predetermined digital code, a trust level which indicates that the certifier warrants that the user named in the certificate is known to the certifier and is certified to use the associated public key. However, by virtue of this digital code, the user ("certifiee") is not authorized to make any further identifications or certifications on the certifier's behalf. Alternatively, the certifier may issue a certificate having other digital codes including a code which indicates that the user of the public key is trusted to

accurately identify other persons on the certifier's behalf and (perhaps) is even further trusted to delegate this authority as the user sees fit.

The present invention further provides for a user's public key to be certified in multiple ways (e.g., certificates by different certifiers). The present invention contemplates including the appropriate certificates as part of a user's signed message. Such certificates include a certificate for the signer's certifier and for the certifiers' certifier, etc., up to a predetermined certificate (or set of mutually referenced co-certificates) which is trusted by all parties involved. When this is done, each signed message unequivocally contains the ladder or hierarchy of certificates and the signatures indicating the sender's authority. A recipient of such a signed message can verify that authority such that business transactions can be immediately made based upon an analysis of the signed message together with the full hierarchy of certificates.

Col. 18, lines 33-68, of Fischer state:

The manner in which a party B creates a certificate for party A is shown in FIG. 5. As indicated at 100, A creates a public/private key pair in accordance with conventional public key signature systems and supplies the public key to B 102. Once B obtains the public key provided by A for certification, it is important for B to insure that the public key is actually one generated by A and not someone masquerading as A. In this regard, it may be desirable for the public key generated by A to be provided on a face to face basis.

Having selected his own certificate with which to sign A's certificate, B at 106 utilizes the certificate 108 with the associated public key 110 to create a signature of a new certificate 112. As in FIG. 2, the signature is created using an object (A's certificate 116) and a certificate (B's certificate 108). B's secret private key is utilized in the decrypt operation to create the signature 112 of the new certificate 116 and the signature packet 114 of B's signature becomes part of A's new certificate packet.

Focusing on the certificate for A which is constructed using information about A specified by B, B builds the certificate by utilizing the public aspect of A's public key as provided by A via line 103. B also sets forth A's full name, A's title and other important statistics such as his address, and telephone number. B may also include a comment to go with the certification which will be available to any person in the future who needs to examine A's certificate.

B additionally will indicate an expiration date of the certificate. This date may reflect the date after which A should not use the certificate. Alternatively, the date may call for any certificate created by A to also expire on this date. B may also indicate in the certificate an account number for A which may represent an internal identification code within B's organization.

As noted above, Fischer is directed to a public key cryptographic system with enhanced digital signature certification. A public key cryptographic system typically includes a public/private key pair. However, both the public and the private key of the key pair in Fischer are active when they are generated. There is no disclosure, teaching or suggestion in Fischer of generating a first cryptographic key pair, and deducting funds from the register for obtaining the requested certificate which activates a first private key of the first cryptographic key pair as is recited in claim 36. The reference to Payne et al. does not overcome this deficiency, as Payne et al. is directed to a conventional network based sales system that utilizes a credit card account to pay for purchases made on-line. There is no disclosure, teaching or suggestion, in Fischer or Payne et al., either alone or in combination, of generating a first cryptographic key pair, and deducting funds from the register for obtaining the requested certificate which activates a first private key of the first cryptographic key pair as is recited in claim 36. The Final Rejection has not provided any basis as to how the passages relied upon disclose, teach or suggest these features.

For at least these reasons, the final rejection of claim 36 is in error and should be reversed.

IX. Conclusion

In Conclusion, Appellants respectfully submit that the final rejection of claims 35 and 36 is in error for at least the reasons given above and should, therefore, be reversed.

Respectfully submitted,

Brian A. Lemm
Reg. No. 43,748
Attorney for the Appellants
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, Connecticut 06484-8000

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Assistant Commissioner for Patents
Washington, D.C. 20231

on April 4, 2003
Date of Deposit

Brian A. Lemm
Name of Registered Rep.

Signature

April 4, 2003
Date

OIPE JC109
APR 1 0 2003
PATENT & TRADEMARK OFFICE

RECEIVED
APR 1 5 2003
GROUP 3600

APPENDIX A

35. A method for obtaining a cryptographic certificate, comprising the steps of:

providing a register having funds stored therein;

determining if sufficient funds are present in the register for obtaining the certificate;

sending a certificate request to a certificate authority;

receiving the cryptographic certificate from the certificate authority; and

deducting funds from the register for obtaining the requested certificate.

36. The method of claim 35, comprising the further steps of:

generating a first cryptographic key pair, wherein said certificate request includes at least a first public key of the first cryptographic key pair; and

activating a first private key of the first cryptographic key pair.